

คู่มือการใช้งาน OpenVas (Greenbone)

Step การใช้งาน OpenVas (Greenbone)

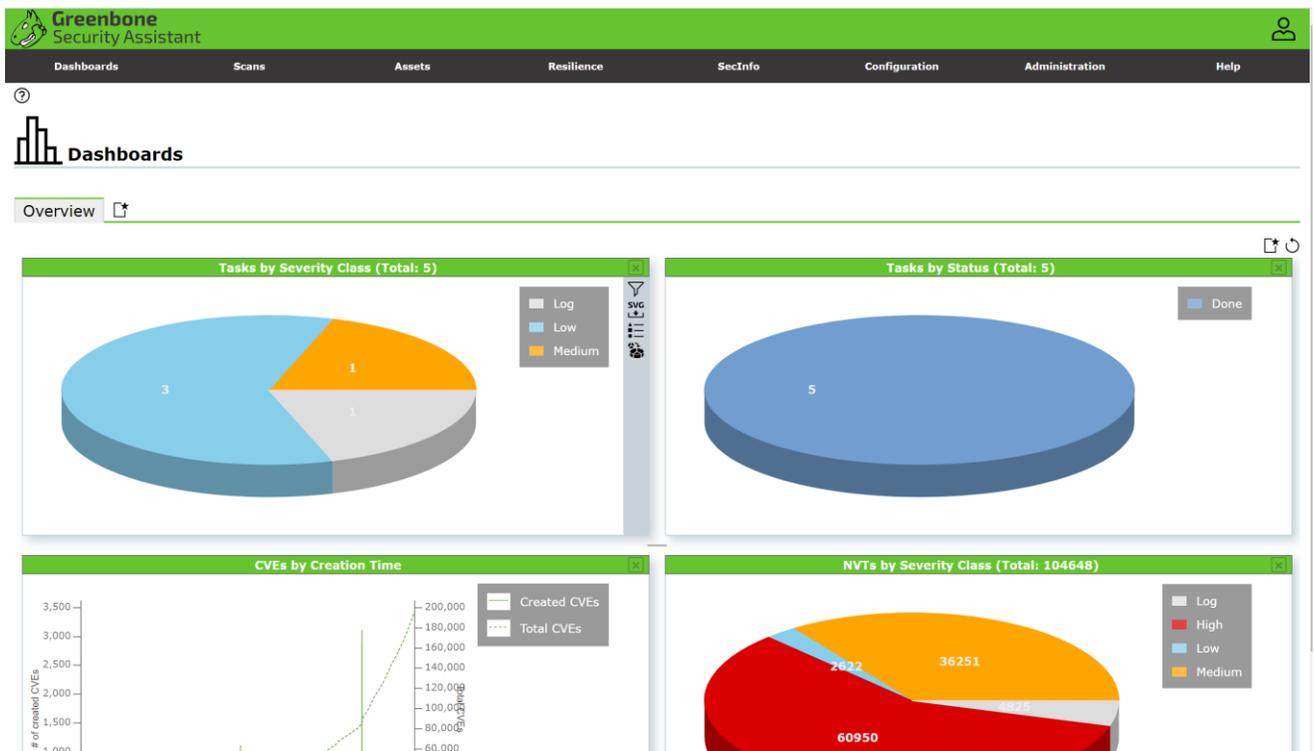
Step 1. ตรวจสอบ Version ของ OpenVas ว่า update ล่าสุดแล้วหรือยัง

Step 2. ทำการสร้าง Targets (สามารถสร้าง Credentials ได้)

Step 3. ทำการสร้าง Tasks และสั่ง Scan (สามารถตั้ง Schedule ในการ Scan ได้)

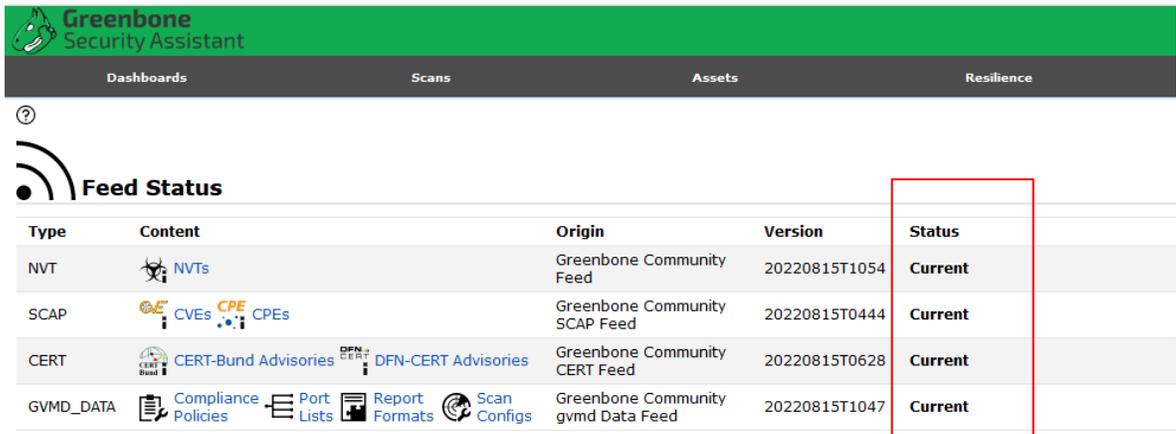
Step 4. เมื่อทำการ Scan เสร็จทำการตรวจสอบผลการ Scan

1. เข้าใช้งานระบบ OpenVas (Greenbone) ผ่าน URL : <https://164.115.35.18:9392/> และทำการ Login ด้วย Username Password ที่ทางทีมทำการส่งให้



2. ทำการตรวจสอบ Version

2.1 เลือกเมนู Administration > Feed Status



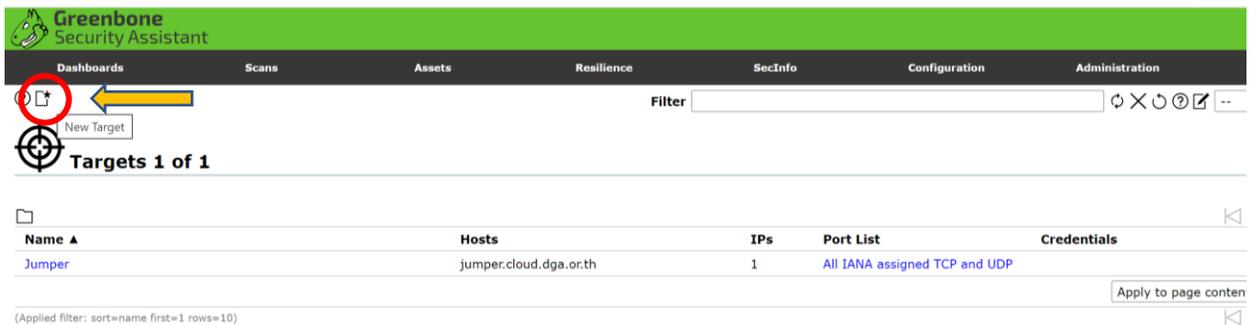
The screenshot shows the 'Feed Status' page in Greenbone Security Assistant. The page has a green header with the logo and a dark navigation bar with tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, and Administration. Below the navigation bar is a search filter and a 'New Target' button. The main content is a table with the following data:

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20220815T1054	Current
SCAP	CVEs, CPEs, CPEs	Greenbone Community SCAP Feed	20220815T0444	Current
CERT	CERT-Bund Advisories, DFN-CERT Advisories	Greenbone Community CERT Feed	20220815T0628	Current
GVMD_DATA	Compliance Policies, Port Lists, Report Formats, Scan Configs	Greenbone Community gvmd Data Feed	20220815T1047	Current

ปล. หาก Status มีการ Update ไปมากกว่า 7 วันให้ทำการแจ้ง Admin

3. ทำการสร้าง Targets

3.1 Configuration > Targets > เลือก New Target



The screenshot shows the 'Targets' page in Greenbone Security Assistant. The page has a green header with the logo and a dark navigation bar with tabs: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, and Administration. Below the navigation bar is a search filter and a 'New Target' button. The main content is a table with the following data:

Name ▲	Hosts	IPs	Port List	Credentials
Jumper	jumper.cloud.dga.or.th	1	All IANA assigned TCP and UDP	

(Applied filter: sort=name first=1 rows=10)

3.2 ทำการกรอก IP ที่ต้องการ Scan

New Target

Name: Unnamed

Comment:

Hosts: Manual **1. ใส่ IP ที่ต้องการ Scan**
 From file No file chosen

Exclude Hosts: Manual
 From file No file chosen

Allow simultaneous scanning via multiple IPs: Yes No

Port List: ALL IANA assigned TCP and UDP **2. เลือก Port List : ALL IANA assigned TCP and UDP**

Alive Test: Scan Config Default **3. เลือก Alive Test : Scan Config Default**

Credentials for authenticated checks

SSH: -- on port 22

SMB: --

ESXi: --

SNMP: --

Reverse Lookup Only: Yes No

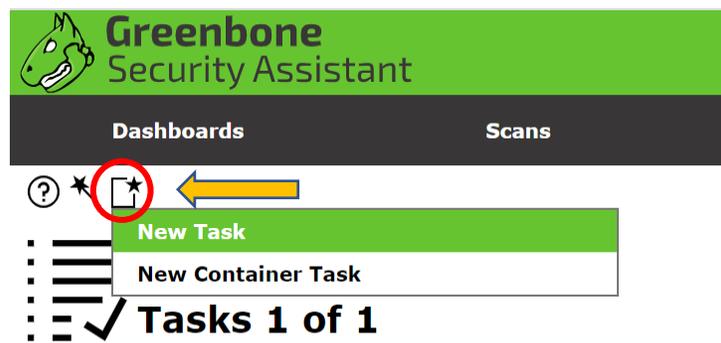
Reverse Lookup Unify: Yes No

4. ทำการ SAVE

หากต้องการใส่ Credentials ให้ทำการสร้างที่เมนู Configuration > Credentials จากนั้นถึงทำการเลือกได้ที่ Credentials for authenticated

4. ทำการสร้าง Tasks และสั่ง Scan

4.1 เลือกเมนู Scans > Tasks > เลือก New Task



4.2 ทำการเลือก Target ที่ได้สร้างไว้ และกรอกข้อมูลการ Scan เพิ่มเติม

New Task
✕

Name 1. ระบุชื่อ Tasks ที่ต้องการตั้ง

Comment

Scan Targets 2. เลือก Targets ที่สร้างไว้

Alerts

Schedule Once

Add results to Assets Yes No

Apply Overrides Yes No

Min QoD %

Alterable Task Yes No

Auto Delete Reports Do not automatically delete reports
 Automatically delete oldest reports but always keep newest reports

Scanner

Scan Config

Network Source Interface

Order for target hosts

Maximum concurrently executed NVTs per host

Maximum concurrently scanned hosts

Cancel
3. กด Save
Save

4.3 ทำการ Scan ทันที

Greenbone Security Assistant
Bo

Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help

Filter

Tasks 1 of 1

Tasks by Severity Class (Total: 1)

Tasks with most High Results per Host

Tasks by Status (Total: 1)

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Jumper	Done	1	Wed, Sep 14, 2022 2:22 PM +07	2.6 (Low)	▲	▶ 🗑️ 🔄

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

4.4 ทำการตั้ง Schedule ในการ Scan

The image shows a software interface for creating a new task. The main window is titled "New Task" and contains several input fields: "Name" (set to "Unnamed"), "Comment", "Scan Targets", "Alerts", and "Schedule". The "Schedule" field is currently set to "--" and has a dropdown arrow and a star icon. An orange callout box with the Thai text "ทำการคลิกที่ Schedule" (Click on Schedule) points to the star icon. A blue arrow points from the star icon to a green button labeled "New Schedule" which is highlighted with a red border. Below the main window, a detailed "New Schedule" dialog is open, showing configuration options: "Name" (Unnamed), "Comment", "Timezone" (Asia/Bangkok), "First Run" (09/26/2022 at 14:00), "Run Until" (09/26/2022 at 15:00 with "Open End" checked), "Duration" (Entire Operation), and "Recurrence" (Once). "Cancel" and "Save" buttons are at the bottom.

New Task

Name: Unnamed

Comment:

Scan Targets: [Dropdown] [Star]

Alerts: [Dropdown] [Star]

Schedule: -- [Dropdown] [Star] **ทำการคลิกที่ Schedule**

New Schedule

Name: Unnamed

Comment:

Timezone: Asia/Bangkok

First Run: 09/26/2022 [Calendar] 14 h 0 m [Now]

Run Until: 09/26/2022 [Calendar] 15 h 0 m Open End

Duration: Entire Operation

Recurrence: Once

Cancel Save

5. ตรวจสอบผลการ Scan

5.1 เลือกเมนู Scans > Reports

The screenshot displays the Greenbone Security Assistant interface. At the top, there is a navigation bar with tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below this is a filter input field. The main content area is titled "Reports 1 of 1" and contains three charts:

- Reports by Severity Class (Total: 1):** A 3D pie chart showing 1 report in the Low severity class.
- Reports with High Results:** A line graph showing Max High and Max High per Host over time (Tue 13, Wed 14). Both values are 0.
- Reports by CVSS (Total: 1):** A bar chart showing the number of reports for each severity level. The bar for severity 2 is at 1.0, and all other bars are at 0.0.

Below the charts is a table with the following data:

Date	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Wed, Sep 14, 2022 2:22 PM +07	Done	Jumper	2.6 (Low)	0	0	1	39	0	△ X

Annotations in the image include a red circle around the date link, a red box around the severity statistics, and an orange box with the text "คลิกเพื่อดูรายละเอียดเพิ่มเติม" (Click to view more details) with an arrow pointing to the date link.

ผลสรุป Severity ที่ Scan เจอ

คลิกเพื่อดูรายละเอียดเพิ่มเติม

5.2 เลือกที่ Results



Report: Wed, Sep 14, 2022 1:54 PM +07 Done

Information	Results (1 of 35)	Hosts (1 of 1)	Ports (0 of 3)	Applications (2 of 2)	Operating Systems (1 of 1)	CVEs (0 of 0)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)
-------------	-----------------------------	-------------------	-------------------	--------------------------	-------------------------------	------------------	-------------------------	------------------------------	----------------------------	------------------

Vulnerability		Severity ▼	QoD
TCP timestamps		2.6 (Low)	80 %



Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Detection Result

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1118975456
Packet 2: 1118976548

Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: [TCP timestamps OID: 1.3.6.1.4.1.25623.1.0.80091](#)

Version used: 2020-08-24T08:40:10Z

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution Type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

References

Other <http://www.ietf.org/rfc/rfc1323.txt>
<http://www.ietf.org/rfc/rfc7323.txt>
<https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152>